Scott Gordon
COMP 5130, Internet and Web Systems I
12/1/2022
Term Paper

A Survey of Data Encryption Technologies

1. Abstract

Network security is an essential component of the internet. Without network security, we would lose all faith that our data is secure and private, and more importantly, we would lose access to many services such as online banking. For these services to have and maintain our trust, they must be consistently updating their protection to account for advances in the field. There are many ways to encrypt our data, and in this paper, we are introducing and comparing some of these technologies.

2. Introduction

Network and data security is very important in a variety of fields, and because of this, many network security technologies are specifically designed to meet the needs of the data that is being encrypted. In this paper, we look at different technologies from different areas of security and compare how well they accomplish their task to see how improvements can be made in each area.

The first encryption algorithm we looked at is a general encryption algorithm that uses public keys to provide an additional type of security outlined in the paper (Sahai & Seyalioglu, 2010). The purpose of this algorithm is to provide an option for encryption in a public key setting where the user does not have to worry about if there is a corrupted certificate authority, or if the user they are sending data to has the proper credentials to accept the data. To accomplish this securely, the authors set out to accomplish four core security guarantees. The security guarantees are as follows: "The scheme should be secure against eavesdroppers" , "The policy of a ciphertext should remain hidden", "A user's public key should leak no information about his credentials", and "Even if the certification authority is corrupted, it should not be able to compromise the security of any encryptions prepared for honest users" (Sahai & Seyalioglu, 2010).

The second encryption algorithm we are looking at is "Length-preserving Bit-stream-based JPEG Encryption" (Unterweger & Uhl, 2012). In this paper, Unterweger and Uhl propose a new method of encryption for JPEGs that avoid recompression. The proposed method uses bit stream encryption to accomplish security, and since this is applied directly to the bitstream, they can cut out steps that other algorithms must take, greatly improving the speed of the algorithm.

The third algorithm we will be considering was proposed by Deng et al. in their paper "Secure and Fast Encryption (SAFE) with Classical Random Number Generators" (DENG et al., 2018). In this paper, Deng et al. mention the problem of predictable and pseudo-random number generators (PRNGs) with statistically expected outcomes. Deng et al. propose a potential solution to this problem with their new method SAFE. The SAFE method combines multiple pseudo-random number generators, inheriting their properties of randomness. They also provide mutual shuffling to avoid linearity in the statistical outcomes of their randomly generated numbers.

The last encryption algorithm we are looking at was proposed by Hashizume and Fernandez in their paper “Symmetric Encryption and XML encryption Patterns”. This paper looks at two patterns, a symmetric encryption pattern that describes most of basic algorithms under that umbrella, and an asymmetric encryption for the purpose of encrypting XML messages. The first pattern, the symmetric encryption is simple and does not require much to go over, but the second pattern, the asymmetric encryption for XML messages is more interesting. Hashizume and Fernandes’ solution to this problem of XML message encryption is to transform the XML message using an asymmetric encryption so that only legitimate users with valid keys can understand the message. In their paper, they recommend using a strong encryption algorithm as the base such as AES and DES for symmetric encryption, or RSA for asymmetric.

3. Overview and Comparison

The technology proposed by Sahai and Seyalioglu provide two primary contributions, the idea of ‘worry-free encryption’ (Sahai & Seyalioglu, 2010), as well as three different proofs of concepts. First, they provide the basic construction for their worry-free encryption. Second, they build on the basic construction to build one that secures the encryption against chosen ciphertext attacks. Lastly, they provide a proof that “if non-interactive zero knowledge proofs for NP exist, there exists IND-CCA2 secure Worry-Free Encryption without random oracles” (Sahai & Seyalioglu, 2010). The first concept details exactly how the algorithm works and shows the benefits. The second concept shows that the original idea can be built upon in meaningful ways with little cost to the runtime. The third concept explains how the worry-free encryption model holds up in a variety of settings. This provides for a versatile and useful algorithm. The primary focus of this paper was to provide a new form a security that is not applicable in all settings but is very useful in the scenarios where it can apply.

The algorithm proposed by Unterweger and Uhl provide a unique method to JPEG encryption. Their method uses swap and scramble operations directly on the bitstream when encrypting and preserves the length while doing so. Because of the encryption applying directly to the bitstream, it is considered faster than other counterparts which also conserve the length. This paper mainly contributes a combination of technologies that, when together, make a meaningful contribution to the speed of existing algorithms. This encryption method is more specific in its use case than Sahai and Seyalioglu’s, but provides an improvement to runtime while Sahai and Seyalioglu’s provides a new technology.

The technology proposed by Deng et al. poses a divide in the available pseudo random number generators (PRNGs). One side, network security, the security is extremely important. On the other side, computer simulation, security isn’t a concern. This side is more focused on things like efficiency, distribution, and portability. In this paper, Deng et al. provide a solution that mixes the two sides to gain the benefits of both. They provide a PRNG that has the efficiency and portability of a computer simulation PRNG while maintaining the security of a network security PRNG. Since random numbers are very useful in many different areas, this algorithm can be very useful. Like Sahai and Seyalioglu’s algorithm, this one also provides a new technology for the security space. This contrasts with Unterweger and Uhl’s contribution, which is a development on an existing technology.

The last technology is introduced by Hashizume and Fernandez. In their paper, they provide a solution to XML message encryption. When coming up with their solution, Hashizume and Fernandez took into account the following four forces: “confidentiality, Convenient reception, Protocol, Performance, and Security” (Hshizume & Fernandez, 2009). There were two patterns offered by the paper, symmetric encryption, and XML encryption. The first to make clearer the logic behind the second. To make it clearer, this paper puts forth a new method of encrypting XML messages that was not offered in the past. This method is more secure than previous methods with comparable speeds. This paper is in the same category as Unterweger and Uhl’s contribution, that being a new technology to add security in an area that was previously missing it.

4. Conclusion

There are many different technologies and algorithms that go into strong network security. To maintain trust in our applications, we must be sure that developers are updating their security to match industry standards, and that these standards are progressing as new technologies are developed. We have gone over four different algorithms and ideas that represent progress in different areas of network security. Some of them making progress on existing ideas, increasing efficiency or security, while others are creating new algorithms to apply data security in areas that previously didn’t have a specific solution. Work like this is important to the field of Internet and Web Systems because data security is an essential part of the internet and our trust in many different applications.

Another main takeaway from this paper is that in addition to new algorithms and technologies, advancements on existing technologies are equally important to the development of the field. While new technologies can contribute to the field in a way that existing technologies cannot, strengthening existing algorithms and making them more efficient are just as essential to the users. Advancements on old algorithms and new unique advancements both share the goal of making the user experience faster and more secure.

5. Future Analysis

In the future, it is important to look deeper into these new or developing technologies to see how well they accomplish their goals when compared to similar algorithms and try to see where else they can be applied. It would be interesting to do a more direct comparison of these algorithms while narrowing the scope as to focus on a more specific, smaller subsection of network security. It would be possible to focus on maybe one of the technologies we brought up in this paper and find more specific alternatives for a better comparison.

6. References

Andreas Unterweger and Andreas Uhl. 2012. Length-preserving bit-stream-based JPEG encryption. In Proceedings of the on Multimedia and security (MM&Sec '12). Association for Computing Machinery, New York, NY, USA, 85–90. https://doi-org.umasslowell.idm.oclc.org/10.1145/2361407.2361421

Amit Sahai and Hakan Seyalioglu. 2010. Worry-free encryption: functional encryption with public keys. In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10). Association for Computing Machinery, New York, NY, USA, 463–472. https://doi-org.umasslowell.idm.oclc.org/10.1145/1866307.1866359

Lih-Yuan Deng, Jyh-Jen Horng Shiau, Henry Horng-Shing Lu, and Dale Bowman. 2018. Secure and Fast Encryption (SAFE) with Classical Random Number Generators. ACM Trans. Math. Softw. 44, 4, Article 45 (December 2018), 17 pages. https://doi-org.umasslowell.idm.oclc.org/10.1145/3212673

Keiko Hashizume and Eduardo B. Fernandez. 2009. Symmetric encryption and XML encryption patterns. In Proceedings of the 16th Conference on Pattern Languages of Programs (PLoP '09). Association for Computing Machinery, New York, NY, USA, Article 13, 1–8. https://doi-org.umasslowell.idm.oclc.org/10.1145/1943226.1943243